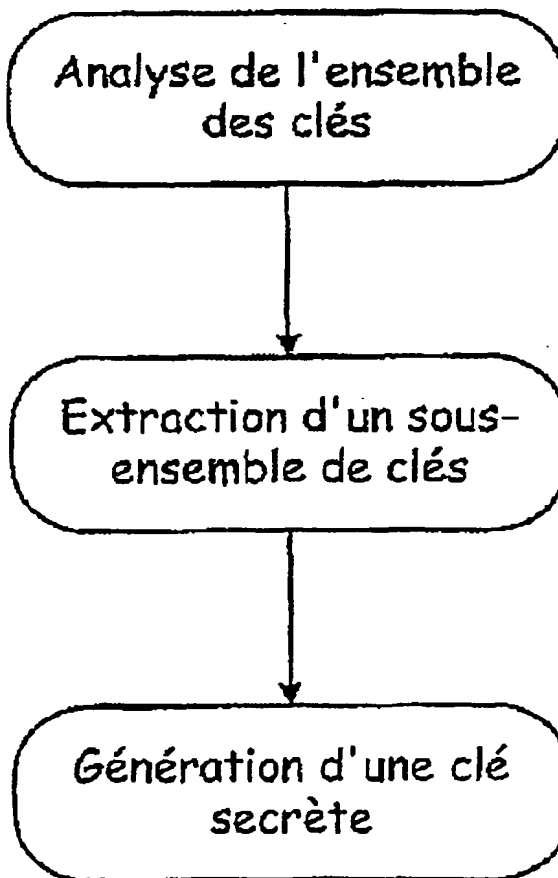


Selection of a secret key at random from a set of possible keys for use in personalization of an electronic component, especially a chip card so that protection against side channel attacks or crypto analysis is improved

Priority number(s): FR20020001883 20020215

 AU2003222888 (A)

Method for generation of secret secure keys for a cryptographic algorithm has the following steps: extraction of a set of possible keys; extraction of a sub-set of keys; and generation of secret keys from a sub-set of keys. The invention also relates to a corresponding device for personalization of an electronic component using a secret key chosen at random from a sub-set of possible keys using the inventive method.



file://C:\Documents%20and%20Settings\user USER_7D762F0C011#302 061711021ED... 2007/5/22